

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date filed: 4/30/09

Name of company(s) covered by this certification: Net 56, Inc.

Form 499 Filer ID: 826832

Name of signatory: Bruce L. Koch

Title of signatory: President

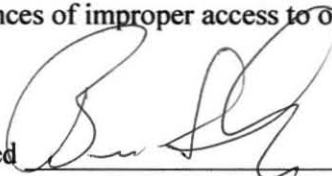
I, Bruce L. Koch, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules, (See attached-Exhibit A)

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed



Bruce L. Koch, President  
Net 56, Inc.

## Exhibit A

### 5. Data Security Policy

- 5.1. Company data is information that supports the mission and operation of Net56, Inc. It is a vital asset and is owned by the Company. Some organizational data may be distributed across multiple departments of the Company, as well as outside entities. Company data is considered essential, and must comply with legal, regulatory, and administrative requirements.
- 5.2. Departments must assess organizational risks and threats to the data for which they are responsible, and accordingly classify its relative sensitivity as Level I (low sensitivity), Level II (moderate sensitivity), or Level III (high sensitivity). *Unless otherwise classified, institutional data is Level II.* Employees may not broaden access to organizational data without authorization from the department responsible for the data. This limitation applies to all means of copying, replicating, or otherwise propagating Company data.
  - 5.2.1. All data shares to be set up between systems must be requested via IT to ensure data integrity.
- 5.3. Data Classification
  - 5.3.1. Authorization to access organizational data varies according to its sensitivity (the need for care or caution in handling). For each classification, several data handling requirements are defined to appropriately safeguard the information. It's important to understand that overall sensitivity of institutional data encompasses not only its confidentiality (need for secrecy), but also the need for integrity and availability. The need for integrity, or trustworthiness, of organizational data should be considered and aligned with organizational risk; that is, what is the impact on the organization should the data not be trustworthy? Finally, the need for availability relates to the impact on the organization's ability to function should the data not be available for some period of time. There are three classification levels of relative sensitivity which apply to institutional data:
- 5.4. Level I: Low Sensitivity

Access to Level I organizational data may be granted to any requester, or it is published with no restrictions. Public data is not considered sensitive. The integrity of "Public" data should be protected, and the appropriate department or unit must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the organization should Level I data not be available is typically low, (inconvenient but not debilitating). Examples of Level I "Public" data include published "white pages" directory information, maps, department, and websites.
- 5.5. Level II: Moderate Sensitivity

Access to Level II organizational data must be requested from, and authorized by, the department who is responsible for the data. Access to internal data may be authorized to individuals based on job classification or responsibilities ("role-based" access), and may also be limited by one's employing department. Non-Public or Internal data is moderately sensitive in nature. Often, Level II data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the Company should this information not be available when needed is typically moderate. Examples of Level II "Non-Public/Internal" organizational data include project information, official Company records such as financial reports, human resources information, and budget information.
- 5.6. Level III: High Sensitivity

Access to Level III organizational data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the Company who require such access in order to perform their job, or to those individuals permitted by law. Access to confidential/restricted data must be individually requested and then authorized by the department or unit who is responsible for the data. Level III data is highly sensitive and may have personal privacy considerations, or may be